The Future of Privacy:

A Consumer-Oriented Approach to Managing Personal Data Online

Siobhan MacDermott and J.R. Smith

AVG Technologies USA, Inc.

Abstract

Beginning with Facebook's recent controversial "tweaks" to its privacy policy and its promise to support users against employers and others who attempt to compel users to divulge passwords, we critically review European Union (EU) and U.S. digital privacy initiatives. Whereas the EU proposal relies on legislative regulation, the U.S. proposes industry self-regulation partially enforceable by the Fair Trade Commission (FTC). We conclude that not only do the sharply differing EU and U.S. approaches present significant problems of global digital interoperability, neither proposal promises to result in practical and feasible consumer protection, at least not in the near term. Moreover, the EU proposal poses serious threats to profitability of digital commerce. As an alternative, we propose a "third approach," empowering the individual digital consumer/user through a personal online strategy we call "wide-open privacy," which provides security without sacrificing the transformative economic, cultural, and personal benefits of the Internet.

Keywords: Consumer Privacy Bill of Rights, data collection, European Union, Facebook, online privacy, privacy legislation, surveillance

"Americans have always cherished our privacy," President Barack Obama wrote in his introduction to *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, a document that contains the administration's proposed "blueprint for privacy in the information age," The Consumer Privacy Bill of Rights. "From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers." Indeed, the president observes, "Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones," and he declares it "incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times" (White House, February 2012).

President Obama's introduction is dated February 23, 2012. Less than a month later, on March 15, intelligence journalist James Bamford published in Wired.Com a story about a massive $2 billion National Security Agency (NSA) facility under construction in the shadow of Utah's Wasatch Range. "Once built," Bamford writes, "it will be more than five times the size of the U.S. Capitol." Its mission: "to intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks."

> Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter." It is, in some measure, the realization of the "total information awareness" program created during the first term of the Bush administration—an effort that was killed by Congress in 2003 after it caused an outcry over its potential for invading Americans' privacy (Bamford, March 15, 2012).

The national cognitive dissonance implied by the government's promulgation of a "Consumer Privacy Bill of Rights" even as it builds a facility dedicated to rendering digital privacy impossible makes it stunningly clear: the fate and future of privacy is a defining issue of our era.

And government is hardly the only source of digital surveillance, intrusion, exploitation, and manipulation. Like it or not, desire it or not, we are all celebrities today. We are all famous or notorious—or may become so at any moment—because everything we do is observable by some government or corporate entity or even by some individual. We each of us publish an extraordinary volume of financial, intellectual, and political personal data, voluntarily if unthinkingly, on e-commerce websites, financial websites, media sharing sites, and social media sites. With far less conscious volition, we also leave our digital footprints everywhere we travel on the Web, as well as in emails, instant messages, texts, and cell phone conversations.

Even if we make a deliberate effort to do little or nothing online to reveal ourselves, we are revealed. Our smartphones are location-tracking devices (whether by GPS, cell phone tower pinging, or both) and also provide data (for example) on our movements, usage and communications, and social proximity to others (by means of Bluetooth monitoring). Remote surveillance can monitor our calls, SMS transmissions, and browser use, as well as the data logs for all of these. Apps, both actually running and merely installed, are subject to monitoring, as are contacts, personal information, and music, image, and video files (funf.org).

Turning off your smartphone provides no guarantee of privacy. According to the U.S. Commerce Department, "a cellular telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone." Software remotely installed by a cell phone service provider can, without the user's knowledge, activate the device's microphone, even when no call is being made. Some phones can be remotely accessed and made to transmit room audio continually. The FBI reportedly used such remote cell phone microphone activation to create "roving bugs" against "members of a New York organized crime family who were wary of conventional surveillance techniques" (McCullagh and Broache, December 1, 2006). Today's smartphones offer not only a microphone but extraordinarily sophisticated video camera features, which can be remotely activated without a user's knowledge. It is also possible to remotely activate the webcam of a laptop or desktop computer without the user's knowledge (Magid, February 22, 2010). Shed your smartphone and unplug your PC, and you are still subject to satellite surveillance, pilotless drones, and fixed-location surveillance cameras that are ubiquitous in buildings and on the streets.

Privacy and its future are issues urgent yet seemingly so vast as to defy cogent let alone actionable discussion. For this reason, we propose to begin by considering a single website,

albeit one with extraordinary reach. We believe that to discuss the *particular* topic of "Facebook privacy" is in fact to address the *general* topic of privacy online. Facebook's business is founded entirely on the user's willingness to share information. This means that Facebook's business is founded on the very core of the Internet, which is, first and last, an information-sharing platform. Ideologically, culturally, and commercially, Facebook may be regarded as the flagship Internet site. We could call it a microcosm of the Web, except that there is nothing "micro" about it. With some 800 million users, the company earned a profit of $668 million in 2011 and booked $3.7 billion in revenue. An anticipated IPO is expected to be valued as high as $100 billion. Most of the money actually made as well as the value widely perceived is derived from ads that target users based on the information they share (Associated Press, March 23, 2012).

An Issue of Semantics

Even the most casual user of Facebook may be stunned by the level of personal, financial, intellectual, and professional information many willingly share with (in many instances) thousands of "friends" and (also in many cases) potentially nearly a billion perfect strangers. That individual *willingness* goes to the heart of Internet privacy, and yet recent efforts by the United States government and the European Union to plan how to regulate, manage, and protect online privacy do not even address it. (We will—at the conclusion of this paper.)

What U.S. and EU officials *have* proposed to address is "promoting the rights of individuals to have their personal data protected" (EU-U.S., March 19, 2012). Yet even in this, they have executed a telling semantic sleight of hand. The joint statement does not commit the governments to promoting rights of protection of personal *privacy,* but of personal *data.*

That word is revelatory, and it is heavily loaded. Let's return to Facebook. The company has long wrestled with privacy issues, and in November 2011 settled with the United States Federal Trade Commission (FTC) over allegations that it had misled users about how it handled their personal information. On March 22, 2012, Facebook posted a draft of its revised "Statement of Rights and Responsibilities" (SRR), which included renaming its "privacy policy" a "data use policy" (Allan, March 24, 2012). This and other so-called "tweaks" to the SRR language triggered many user protests, including postings by more than 30,000 German users who rejected the proposed changes en masse.

Arguably—and paradoxically—what the disgruntled users were unwittingly protesting was Facebook's efforts to be honest, straightforward, and transparent. The revised language may well have been an earnest attempt to avoid a repetition of last year's charges of misleading users. The truth is that, like any other Internet site based on sharing information, Facebook cannot reasonably promise to protect "privacy"—since privacy depends on what users choose to share and choose to guard—and can only sincerely undertake to protect "data." Unfortunately for both Facebook's public image and the naïveté of many users, this semantic transparency exposes an inevitable gap between *privacy* (a moral construct that can be created or destroyed by individual actions) and *data* (a morally neutral arrangement of bits and bytes). When we commit private thoughts, feelings, or facts to paper, to silicon, or to the cloud, they become neither thoughts, nor feelings, nor facts. They become data.

Like the governments of the EU and the U.S., Facebook proposes to promote the protection of personal data, but it *is* data nevertheless, no matter how much many of us wish it would remain special, individual, human, and private, which is to say sacred. Silicon is not a sanctuary, however, and the cloud is not heaven. On the Web, all is data.

Facebook, like other commercial websites, monetizes data. In a recent article, Alexis Madrigal, a senior editor at *The Atlantic,* pointed out that online user profiles are sold to advertisers and marketers for half a cent per profile (at the high end), which means that "Facebook and Google make roughly $5 and $20 per user, respectively" and the whole of the "Internet advertising ecosystem" generates something like $1,200 per user profile (Madrigal, March 19, 2012). From an individual perspective, privacy, even when represented as data, is of inestimable emotional, intellectual, and moral value. From the perspective of the Internet advertising ecosystem, this same data costs just half a penny but ultimately goes for $1,200 a pop.

Either way, privacy—represented as data—is a treasure. For Facebook and the other constituents occupying the Internet advertising ecosystem, the treasure is infinite, *provided that* users remain willing to share personal information. This means websites that collect and use such information have an urgent interest in guarding the treasure both for its value to the individual and for its value to commerce. Facebook acted in just such a spirit when, on March 23, 2012, Erin Egan, the company's "chief privacy officer, policy," issued a statement concerning "a distressing increase in reports of employers or others seeking to gain inappropriate access to people's Facebook profiles or private information."

> The most alarming of these practices is the reported incidences of employers asking prospective or actual employees to reveal their passwords. If you are a Facebook user, you should never have to share your password, let anyone access your account, or do anything that might jeopardize the security of your account or violate the privacy of your

> friends. We have worked really hard at Facebook to give you the tools to control who sees your information. . . .
>
> We don't think employers should be asking prospective employees to provide their passwords because we don't think it's the right thing to do. But it also may cause problems for the employers that they are not anticipating. For example, if an employer sees on Facebook that someone is a member of a protected group (e.g. over a certain age, etc.) that employer may open themselves up to claims of discrimination if they don't hire that person (Egan, March 23, 2012).

Egan's statement went on to promise, "We'll take action to protect the privacy and security of our users, whether by engaging policymakers or, where appropriate, by initiating legal action, including by shutting down applications that abuse their privileges" (Egan, March 23, 2012). As Matt Brian of *The Next Web* reported, "the company is willing to go to bat for users that feel they have been wronged by an employer, which could go as far as filing lawsuits against the companies involved" (Brian, March 23, 2012).

Facebook's stand has been praised both as a brilliant PR move and as a noble blow struck in the defense of online ethics and individual freedom. It is, of course, also an act of enlightened self-interest, and, as such, has another semantic basis. As much as, if not more than, any other commercial website, Facebook depends on users' willingness to share information. Facebook took heat for being honest about the use of the word *data* in preference to *privacy.* Clearly, Facebook's leadership also understands the meaning of the word *share.* The verb implies free will, decision, and choice. It is emphatically not a synonym for *relinquish, lose, give up,* or *abandon*—which is what employers and others who would extort a user's password demand. Allow user data to be extorted or stolen or otherwise forcibly surrendered, and who will continue

to willingly *share*? Stop sharing, and Facebook closes up shop. Whither the flagship goes, so goes the fleet.

Regulation

Before interactive media began in earnest to eclipse mass broadcast media during the mid-1990s, government regulation of "communications" was relatively simple. In the United States, for example, the regulatory authority of the Federal Communications Commission (FCC) rested on the principle that the "airwaves" were a public interest and that, therefore, the limited availability of broadcast bandwidth, a public resource, had to be federally administered to protect and to serve the public good. Until nearly the end of the twentieth century, local broadcast television channels were relatively few, and truly national TV networks were only three. FCC monitoring of so compact a group was feasible, so feasible, in fact, that broadcasters created organizations to avoid government intervention by policing themselves.

While the relatively contained scope of mass-media broadcasting helped make government and industry oversight practical and effective, even more important was the fact that radio and television were one-way media. Broadcasters were the producers, whereas viewers were the consumers. Only the producers received regulatory attention, whether by government, industry organizations, or the corporate sponsors who ultimately financed all programming. In contrast, interactive media is two-way. Every entity that uses the Internet is both a producer and a consumer. Even if, as an individual, you do not create a website, offer anything for sale online, or write a blog, you produce data—by some calculations (as we have seen) at least $1,200 worth.

Whereas three fully national networks exclusively plied the broadcast television airwaves during the second half of the twentieth century, today the Internet hosts billions of consumer-producers. Everything from basic communication, to commerce, to entertainment, to government administration, to social interaction, to the creation, sharing, and dissemination of knowledge takes place on this platform. As recent events in the Arab world and elsewhere have demonstrated, entire governments rise and fall by dint of the Internet.

The value at stake—the "public good"—is certainly incalculable, but just as surely has never been higher. We do have tangible statistics on the cost of identity theft. At present, one out of ten U.S. consumers has been a victim. In 2008, more than 35 million corporate and government data records were compromised by security breaches. Phishing—using the Internet and email to dupe people into revealing personal, especially financial, information—has cost consumers an estimated $1.2 billion to date (VentureBeat, February 2012).

The cost of non-criminal analogues of identity theft—that is, the collection and use of personal data without the knowledge or permission of the "owner" of that data—probably cannot be calculated. But just consider that, until it reached an agreement with the FTC in 2010, Facebook routinely compiled user information even from people who were not members of Facebook. This occurred whenever a non-member user visited a website that featured the familiar Facebook thumbs-up "Like" button. It was not even necessary for that visitor to click the button. As Rob Shavell, cofounder of the online security company Abine, commented, the buttons worked "like a dark video camera—you see them, they see you." By 2010, these buttons were on nearly a million websites (VentureBeat, February 2012).

While the "dark video camera" functionality of Facebook "Like" buttons has been discontinued, Internet users are still exposed to data mining by cookies, which function to

exchange information between the user's computer and a website. About half of the Web's most popular sites use cookies, and at many sites they are required to enable user interaction. Third parties, such as advertisers and marketers, place cookies on some websites to enable them to track browsing information through other websites. While most cookies store user and browsing information for only the duration of the browsing session, 18.5 percent are termed "persistent cookies" and store information indefinitely (VentureBeat, February 2012).

The value of Internet data may be incalculably great and the threats commensurately sinister, but the growth and volume of Internet traffic, the varied nature of that traffic, and the expectation of freedom and openness among users have all outpaced government efforts at regulation.

The EU Approach: Government-Centered

On January 25, 2012, the European Commission's Directorate-General for Justice (DG JUST) presented its proposal for a "Regulation" that is set to replace the EU's existing 1995 Data Protection Directive. Aimed at strengthening the rights of "data subjects" (i.e., Internet users), the new legislation requires "data controllers" (i.e., mostly website owners) to provide more transparent and accessible information to data subjects and to be more responsive to individual requests for personal information. The legislation asserts a right of EU citizens "to be forgotten"—thereby obliging data controllers to delete personal data on request—and a right to data portability. A data controller is prohibited from collecting data from a subject unless the subject gives "explicit" consent, which the subject may subsequently withdraw at any time. A strict opt-in approach for consumers to explicitly allow the placement of every tracking cookie is

part of the proposed legislation, and the formulation of "do not track" (DNT) standards is set to be proposed by June 2012

The EU's government-centered approach raises serious questions of public and corporate costs, feasibility, and the prospect of cumbersome regulation inhibiting the overall growth of the Internet. In particular, businesses that rely on consumer profiling and targeted advertising are likely to suffer widespread, possibly profound, disruption.

There is another problem. In contrast to the EU's government-centered approach to regulation, the United States has proposed precisely what the EU has explicitly rejected: industry self-regulation. As it stands, this difference of approach threatens the global interoperability of Internet commerce, perhaps of the Internet itself.

The U.S. Approach: Industry-Centered

In February 2012, the White House released *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (White House, February 2012). The framework consists of four elements:

1. A Consumer Privacy Bill of Rights
2. "A multistakeholder process to specify how the principles in the Consumer Privacy Bill of Rights apply in particular business contexts"
3. Proposals for strengthening FTC enforcement
4. A "commitment to increase interoperability with the privacy frameworks of our international partners."

The Consumer Bill of Rights is not legally prescriptive, but instead "provides general principles that afford companies discretion in how they implement them." The flexibility is intended to promote innovation and "encourage effective privacy protections by allowing companies, informed by input from consumers and other stakeholders, to address the privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single, rigid set of requirements" (White House, February 2012).

The "multistakeholder process" is aimed at producing "enforceable codes of conduct that implement the Consumer Privacy Bill of Rights" (White House, February 2012). Private sector participation will be voluntary, and companies will choose whether or not to adopt a given code of conduct.

The FTC will enforce whatever "privacy commitments" a company voluntarily makes. That is, while the commitment is voluntary, adhering to the commitment that is made will be sanctioned by the FTC, which, if Congress passes appropriate legislation, will also have "specific authority to enforce the Consumer Privacy Bill of Rights" (White House, February 2012).

Finally, recognizing that the U.S. industry-centered approach is radically different from the EU's government-centered approach, the framework commits to "multistakeholder processes [to] provide scalable, flexible means of developing codes of conduct that simplify companies' compliance obligations" globally (White House, February 2012).

The Third Approach: Your Data, Your Brand

If the EU's government-centered approach to protecting personal data raises grave doubts as to public and private costs, possible impediments to trade, potential inhibition of innovation, and difficulties with global interoperability, the White House "Framework" must strike any candid

reader as far more aspirational than definitively executable, especially with regard to its combination of voluntary codes subject to compulsory FTC enforcement.

Writing in the *New York Times,* technology reporter Steve Lohr observed, "An individual's actions . . . are rarely enough to protect privacy in the interconnected world of the Internet" (VentureBeat, February 2012). It is true. There is no question that good governments will have to find new ways to do in the digital realm what good governments have always sought to do elsewhere: to protect the rights, lives, and property of citizens while simultaneously promoting their welfare, which means (in part) enacting laws that promote rather than impede economic and cultural development. We believe, however, that anyone who impartially evaluates the EU "Regulation" and the U.S. "Framework" will find neither one close to practical readiness for effective implementation.

Much work needs to be done by both the Europeans and the Americans. In the interim, we propose a third approach, one that is truly global precisely because it is most diverse in its application. Instead of concentrating regulation in government or in commercial corporate entities, we propose a strategy that puts it in the hands of individual users of the Internet.

This "third approach" is neither a techno-libertarian call to abandon government nor a cynical denial of the moral and ethical utility of enlightened corporate self-interest. Government regulation and industry codes of conduct should play a role—almost certainly will have to play a role—in something as all-encompassing as the conduct of human affairs on the Internet. Nevertheless, these are *human* affairs, and it is with the individual, with each *human* node on the network, that effective and practical Internet regulation must both commence and culminate.

No technology is more liberating than that of the Internet. Its overall effect is to radically reduce friction in virtually every social, creative, intellectual, political, and economic activity.

But as all people accustomed to democratic government understand, with liberty for all comes the necessity for discipline of the self. Put another way, the greater the freedom, the greater the need for a disciplined approach to that freedom. No technology in the history of civilization has demanded a greater degree of self-regulation than the Internet.

Basic Tools

In Facebook's statement of March 23, 2012, privacy officer Erin Egan not only promises the company's legal support for users from whom employers, prospective employers, or others attempt to extort access to profiles, pages, or other personal data on Facebook, but also advises users to take individual responsibility for their own security and privacy by understanding that "they have a right to keep their password to themselves" (Egan, Erin, March 23, 2012).

Creating strong passwords and keeping them secure is an Internet user's most basic privacy tool. There are others, of course, including:

- Changing your passwords frequently
- Securing mobile devices (not just personal computers) with passwords
- Exercising caution about what software you download to your computer and what apps you authorize on your smartphone
- Installing reliable anti-virus, anti-malware, and do-not-track (DNT) software
- Creating at least two email accounts: one for people and companies you trust and regularly do business with; another for everyone and everything else
- Turning on cookie notices in your browser

- Making use of all the security measures available to you, such as bank and credit card email alerts of unusual activity in your accounts
- Logging off of any public computer you happen to use
- Actually *reading* the privacy policies of websites you use, paying especially close attention to any heading containing the phrases "third parties" or "data collection"

Broader Strategy

Beyond acquiring and using the basic tools of Internet security, we recommend formulating a broader personal strategy aimed at achieving for yourself what the White House hopes to achieve for all users of the Internet: the protection of privacy while making the most of the global digital economy.

The safest strategy with regard to the Internet is to unplug your computer. That will protect privacy all right, but it will certainly not allow you to make the most of the global digital economy. A better alternative is to emulate what great and successful businesses have done for centuries. Create a brand—in the case of the Internet, an online identity designed to present you to the world as you want to be seen by it, as you want it to deal with you.

Wide-Open Privacy

For a company, a brand is proprietary—private—yet also public. The more it is recognized, the more successful it is. Likewise, the most effective and productive users of the Internet present themselves as privately public or publicly private. They achieve what we might call wide-open privacy, becoming fully connected to all of the Internet's frictionless freedom, yet exercising sufficient self-discipline to preserve as sacred whatever data they choose not to share.

Today, people in all walks of business and life must proactively and strategically build and protect their own personal online brands. The idea: If you don't build and protect your own digital brand, someone else will do it for you—or it will be built accidentally, haphazardly, or inconsistently.

Over the next decade, people must do what the managers of successful companies and products do: prioritize, invest in, and discipline their own brand building. This means playing offense in constructing your own digital profiles and in all your Web communications. Figuratively, this means building and maintaining your own "Web site" in every interaction on the Internet. Here is what we mean:

- **Define Yourself**: So that others will not define you. What is especially important is to create your own Web presence, including in all online communications to more trusted people in your network, in which you continually and consistently define the values and character that go into your work and life.

- **Define Your Space:** What do you stand for? What's important to you? And why? Best that you define this in your own publicly private/privately public "branded" digital space so that you can communicate this when and where you wish—and on your *own* terms.

- **Define the Future:** This is what great leaders must do and, more and more, it is what everyday citizens must also do around the world. Define your own "destination"—where you see the future and where you are contributing to make this vision a reality.

The cardinal rule of building an online personal brand is the cardinal rule of all successful marketing: *The person (or company) who controls the dialogue wins!*

Building and protecting your own digital brand follows six key actions:

1. Assume Brand Is Everything: Today, your digital brand must be everything you do. It's not just a Facebook profile, a stream of tweets, a logo, or an email. Your brand is every experience and interaction others have with you on the Web—and in some cases off the Web as well. So the first step in building your online brand is to understand that it consists of everything you do. And, online, everything you do is magnified and multiplied potentially many fold.

2. Differentiate Your Brand: There is no digital value in sameness. Value is created by scarcity, by being different than others. So we all have to differentiate to create digital value for our brand, because, across the Web, users must navigate their choices, and your differentiation is what will help determine user decisions, bring more digital users productively to your brand, thereby enhancing its value and further establishing the online identity you are creating.

3. Know Your Audiences: Just as a business must know as much as possible about its customers, you, an individual, must know your digital audience. In many ways, your connections, fans, friends, and e-mail recipients are your most precious assets in establishing a productive publicly private/privately public online presence. So you must

do what you can to target your "more loyal fans" first, followed by your more extended audiences. Moreover, you must be on a constant learning mission to know more and more about all of these people. In fact, almost always, if you know your digital audiences, they will tell you what you need to be doing online.

4. Communicate Relentlessly: It is not enough just to know your digital audiences. You must also communicate with them. Talk to people, and really listen to them. Engage with them in an interactive digital dialogue. Find out what they are saying about you, because your name is your brand label. And then, discipline communication—once a week, once a month, once a quarter—to help define what your personal brand is and how it is different.

5. Build A Plan: You need a plan to build your own online brand. This means thinking through everything you are doing. Who are the audiences you are trying to reach? Where do you find them? How do you best interact with them? First, know your audiences. Second, understand what they are saying about you. And third, differentiate your online brand. Everything should fit together in the context of a plan and not just amount to a bunch of random, unrelated online activities, which, unfortunately, precisely describes the online presence of most Internet users.

6. Finally, Don't Stop: Your digital brand must always be on the move. Be ready to adjust your game plan as needed. The digital realm is dynamic; therefore, you cannot allow your personal online brand to become static. If you do, others as well as the evolving context of events will change and deform it without your control, let alone

permission. So bring new innovations, new differentiation, and new ways to show new expertise and add new value to your key audiences.

From the perspective of the consumer, the individual, *wide-open privacy* is the most effective—at present, we believe, the *only* effective—model for practical, productive, and secure Internet privacy. The key is to fully embrace the *interactive* in "interactive media." If you want to be passive and safe, unplug. If, however, you want to be practical, productive, and secure online, play offense rather than rely on defense. Everything you place (or merely leave) on the Internet becomes data, no matter how *personally* valuable or sensitive. The most effective means you possess to differentiate your data from the rest, to manage and to direct it so that others use it in ways that are productive and secure for you, is to develop, protect, and evolve your personal online brand just as vigilantly as any proud company builds, guides, and cherishes its brand.

Reference List

Allan, D. (March 24, 2012). "Facebook to Digest Feedback over Controversial Privacy Policy Update." *ITProPortal.* Retrieved from http://www.itproportal.com/2012/03/24/facebook-to-digest-feedback-over-controversial-privacy-policy-update/.

Associated Press (March 23, 2012). "Facebook Addresses More Privacy Concerns; User Doubts Are Still Biggest Threat to Growth," *The Washington Post with Bloomberg Business.* Retrieved from http://www.washingtonpost.com/business/technology/facebook-

addresses-more-privacy-concerns-user-doubts-are-still-biggest-threat-to-growth/2012/03/23/gIQAjDBfWS_story.html?tid=pm_business_pop.

Bamford, J. (March 15, 2012). "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)." Wired.Com. Retrieved from http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

Brian, M. (March 23, 2012). "Facebook Says It May Launch Legal Action against Employers Who Ask for User Passwords." *The Next Web.* Retrieved from http://thenextweb.com/socialmedia/2012/03/23/facebook-says-it-may-launch-legal-action-against-employers-who-ask-for-user-passwords/.

Egan, E. (March 23, 2012). "Protecting Your Passwords and Your Privacy." *Facebook and Privacy.* Retrieved from http://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057.

EU-U.S. (March 19, 2012). "Joint Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson." PRNewswire via COMTEX.

funf.org. Website at www.funf.media.mit.edu.

Hill+Knowlton Strategies (February 2012). "Proposed Reform to the European Data Protection Network: An Analysis of Key Aspects and Suggestions for an AVG Technologies Position Paper." Privately commissioned by AVG Technologies USA, Inc.

Madrigal, A. (March 19, 2012), "How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200." *The Atlantic.* Retrieved from

http://www.theatlantic.com/technology/archive/12/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1200/254730/

Magid, L. (February 22, 2010). "Many Ways to Activate Webcams sans Spy Software." *CNET News*, February 22, 2010. Retrieved from http://news.cnet.com/8301-19518_3-10457737-238.html.

McCullagh, D., and A. Broache (December 1, 2006). "FBI Taps Cell Phone Mic as Eavesdropping Tool." *CNET News*, December 1, 2006. Retrieved from http://news.cnet.com/2100-1029_3-6140191.html.

VentureBeat (February 2012). "Wrestling Online Privacy." Retrieved from http://venturebeat.files.wordpress.com/2012/02/120202onlineprivacy.jpg.

White House (February 2012). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* Retrieved at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.